AGRÉGATION INTERNE
DE MATHÉMATIQUES

épreuve 1

6 heures

– Introduction et notations –

On désigne par E un espace vectoriel euclidien de dimension $n \geqslant 1$.
Si x et y sont deux vecteurs de E, on note $x.y$ leur produit scalaire et $\|x\| = \sqrt{x.x}$ la norme associée.
Un réseau Λ de E est une partie de E vérifiant la propriété suivante :
*il existe une base $\mathscr{B} = (e_1, \dots, e_n)$ de E telle que Λ soit l'ensemble des combinaisons linéaires **à coefficients entiers** des éléments de $\mathscr{B}$:*

$$\Lambda = \left\{ x \in E \;/\; \exists (x_1, \dots, x_n) \in \mathbf{Z}^n,\, x = \sum_{i=1}^{n} x_i e_i \right\}$$

On dit alors que Λ est le réseau défini par la base $\mathscr{B}$, et que $\mathscr{B}$ est une $\mathbf{Z}$-base de Λ.

Soit $u : E \to F$ une application linéaire, F étant un espace euclidien dont on note $< x, y >$ le produit scalaire.
On dit que u est une *isométrie* si, pour tous $x, y \in E$, on a $x.y =< u(x), u(y) >$, et que u est une *similitude* s'il existe une isométrie $v : E \to F$ et un nombre réel $\lambda > 0$ tel que $u = \lambda v$.

Si Λ est un réseau de E et Λ' un réseau de F, on dit que Λ et Λ' sont *semblables* s'il existe une similitude $u : E \to F$ telle que $u(\Lambda) = \Lambda'$.

On désigne par $\mathrm{GL}_n(\mathbf{Z})$ l'ensemble des matrices M d'ordre n à coefficients dans $\mathbf{Z}$, inversibles dans $\mathcal{M}_n(\mathbf{R})$ et dont l'inverse M^{-1} est également à coefficients dans $\mathbf{Z}$.

On rappelle enfin la formule suivante : si Ω, $\mathscr{B}$, $\mathscr{B}'$ sont trois bases de E, on a

$$\det_{\Omega} \mathscr{B}' = \det_{\Omega} \mathscr{B} . \det_{\mathscr{B}} \mathscr{B}'.$$

– Partie A –

On considère dans cette partie un réseau Λ de E, et $(e_1, \dots, e_n)$ une $\mathbf{Z}$-base de Λ.

1. (a) Soit $M \in \mathrm{GL}_n(\mathbf{Z})$; montrer que $\det M = \pm 1$.

(b) Soit M une matrice à coefficients dans $\mathbf{Z}$ telle que $\det M = \pm 1$. Montrer que M appartient à $\mathrm{GL}_n(\mathbf{Z})$ (on pourra considérer la transposée de la comatrice de M).

(c) Montrer que $\mathrm{GL}_n(\mathbf{Z})$ est un sous-groupe du groupe multiplicatif $(\mathrm{GL}_n(\mathbf{R}), \times)$.

2. Vérifier que Λ est un sous-groupe de $(E, +)$.

3. Montrer que deux bases $\mathscr{B}$ et $\mathscr{B}'$ de E définissent le même réseau Λ si et seulement si la matrice de passage P de $\mathscr{B}$ à $\mathscr{B}'$ appartient à $GL_n(\mathbf{Z})$.

4. On suppose dans cette question que $n = 2$ et on note $\mathbf{Z}^2$ le réseau dont une $\mathbf{Z}$-base est la base canonique $(\varepsilon_1, \varepsilon_2)$ de $\mathbf{R}^2$. Soit $x = a\varepsilon_1 + b\varepsilon_2$ un vecteur de $\mathbf{Z}^2$ avec a et b deux entiers premiers entre eux.

(a) Montrer qu'il existe un vecteur y de $\mathbf{Z}^2$ tel que (x, y) est une $\mathbf{Z}$-base du réseau $\mathbf{Z}^2$.

(b) Construire une telle base lorsque $x = 101\varepsilon_1 + 49\varepsilon_2$.

(c) Dans le cas général où $x = a\varepsilon_1 + b\varepsilon_2$ avec a et b deux entiers premiers entre eux, écrire un algorithme permettant de trouver les coordonnées d'un vecteur y tel que (x, y) est une $\mathbf{Z}$-base de $\mathbf{Z}^2$.

(d) Soit $\Lambda = \{x_1\varepsilon_1 + x_2\varepsilon_2 \;;\; (x_1, x_2) \in \mathbf{Z}^2 \;;\; x_2 \equiv x_1 \bmod 3\}$. Montrer que Λ est un réseau de $\mathbf{R}^2$ (on en exhibera une $\mathbf{Z}$-base).

5. Soit $\mathscr{B}$ une $\mathbf{Z}$-base de Λ et Ω une base orthonormale de E. Montrer que $|\det_\Omega \mathscr{B}|$ ne dépend ni de la $\mathbf{Z}$-base $\mathscr{B}$ de Λ ni de la base orthonormale Ω de E.
Ce nombre ne dépendant donc que du réseau Λ, on le note : $\det \Lambda$.

6. (a) Montrer qu'il existe un nombre réel $A > 0$ tel que, pour tout $x = \sum_{i=1}^{n} x_i e_i$ de E, on a
$$A \max_{1 \leqslant i \leqslant n} |x_i| \leqslant ||x||.$$
(b) En déduire que toute boule $\{x,\ ||x|| \leqslant R\}$ centrée en l'origine et de rayon $R > 0$ ne contient qu'un nombre fini de vecteurs de Λ.
(c) En déduire que $m(\Lambda) = \inf_{x \in \Lambda, x \neq 0} \|x\|$ est un réel strictement positif et qu'il existe un vecteur $x_0 \in \Lambda$ tel que $m(\Lambda) = \|x_0\|$.
(d) On désigne par $S(\Lambda)$ l'ensemble $\{x \in \Lambda \ / \ \|x\| = m(\Lambda)\}$. Montrer que $S(\Lambda)$ est fini, puis que $\operatorname{Card} S(\Lambda)$ est un entier pair et non nul.

7. On suppose que $u_1, \dots, u_k$ sont k vecteurs de Λ tels que, pour tout $x \in \Lambda$, il existe $(x_1, \dots, x_k) \in \mathbf{Z}^k$ unique tels que $x = \sum_{i=1}^{k} x_i u_i$. Montrer que $k = n$ et que $(u_1, \dots, u_k)$ est une base de E (on pourra considérer le $\mathbf{Q}$-espace vectoriel engendré par $(e_1, \dots, e_n)$).

8. Soit $D_1 = \mathbf{R}e_1$ la droite engendrée par e_1.
Montrer que $D_1 \cap \Lambda = \mathbf{Z}e_1$.
On suppose que $n \geqslant 2$. Soit F un supplémentaire de D_1 dans E, et p la projection de E sur F parallèlement à D_1. Montrer que $\Lambda' = p(\Lambda)$ est un réseau de F, de $\mathbf{Z}$-base $(p(e_2), \dots, p(e_n))$.
Soit réciproquement $(u'_2, \dots, u'_n)$ une $\mathbf{Z}$-base de Λ', et $(u_2, \dots, u_n)$ des éléments de Λ tels que $p(u_2) = u'_2, \dots, p(u_n) = u'_n$. Montrer que $(e_1, u_2, \dots, u_n)$ est une $\mathbf{Z}$-base de Λ.

9. On note $\varphi_1 : E \to \mathbf{R}$ la forme linéaire qui à tout vecteur $x_1 e_1 + \cdots + x_n e_n$ de E associe x_1 et on pose $F_1 = \ker \varphi_1$.
Soit G un sous-groupe de Λ distinct de $\{0\}$.
(a) Montrer qu'il existe $a_1 \in \mathbf{Z}$ tel que $\varphi_1(G) = a_1 \mathbf{Z}$.
(b) En déduire que, si $n = 1$, G est un réseau de E.
(c) On suppose $n \geqslant 2$, et on note Λ_1 le réseau de F_1 de $\mathbf{Z}$-base $(e_2, \dots, e_n)$. On considère $H = G \cap F_1$. Montrer que H est un sous-groupe de Λ_1.
(d) On suppose $a_1 \neq 0$; soit $b \in G$ tel que $\varphi_1(b) = a_1$. Montrer que, pour tout x de G, il existe un unique couple $(m, v) \in \mathbf{Z} \times H$ tel que $x = mb + v$.
(e) En déduire qu'il existe un sous-espace vectoriel F de E tel que G est un réseau de F (on pourra raisonner par récurrence sur n, en distinguant les cas $G \subset F_1$ et $G \not\subset F_1$).

10. Soit $b = r_1 e_1 + \cdots + r_n e_n$ un élément de $S(\Lambda)$.
(a) Soit k un entier $\geqslant 2$. Montrer que $\frac{1}{k} b$ n'est pas un élément de Λ.
(b) En déduire qu'il existe $s_1, \dots, s_n \in \mathbf{Z}$ tels que $r_1 s_1 + \cdots + r_n s_n = 1$.
(c) Soit $f : E \to \mathbf{R}$ la forme linéaire sur E définie par $f(x_1 e_1 + \cdots + x_n e_n) = s_1 x_1 + \cdots + s_n x_n$. Montrer que $f(\Lambda) = \mathbf{Z}$, que $H = \Lambda \cap \ker f$ est un sous-groupe de Λ et que tout élément de Λ s'écrit de façon unique sous la forme $ab + u$, avec $u \in H$ et $a \in \mathbf{Z}$.
(d) Montrer qu'il existe une $\mathbf{Z}$-base de Λ contenant le vecteur b.

(e) On suppose $n \geqslant 2$. Soit F l'orthogonal de la droite $\mathbf{R}b$ engendrée par b, et p la projection orthogonale de E sur F. Montrer que $p(\Lambda)$ est un réseau de F.

– Partie B : Réseaux et matrices de Gram –

Soit $\mathscr{E} = (e_1, \ldots, e_n)$ un système de n vecteurs de E. On appelle matrice de Gram associée à $\mathscr{E}$ la matrice définie par les produits scalaires : $G = (e_i.e_j)_{i,j} \in \mathcal{M}_n(\mathbf{R})$. Soit une base orthonormale $\Omega = (\omega_1, \ldots, \omega_n)$ de E et $M = (m_{ij})$ la matrice de $\mathscr{E}$ sur Ω (les colonnes de M contiennent les composantes des vecteurs e_j dans la base Ω).

1. Montrer que $G = {}^tMM$. En déduire que $\mathscr{E}$ est une base de E si et seulement si $\det G \neq 0$.

2. Soit un réseau Λ de E, muni d'une $\mathbf{Z}$-base $\mathscr{E}$ de matrice de Gram G. Montrer que

$$\det G = (\det \Lambda)^2.$$

3. Soit $\mathscr{B} = (b_1, \ldots, b_n)$ une famille de n vecteurs d'un réseau Λ.
Montrer que $\mathscr{B}$ est une $\mathbf{Z}$-base de Λ si et seulement si $|\det_\Omega \mathscr{B}| = \det \Lambda$.

4. Soient Λ un réseau de E, F un espace euclidien, et Λ' un réseau de F.

(a) Montrer qu'il existe une isométrie $u : E \to F$ telle que $\Lambda' = u(\Lambda)$ si et seulement s'il existe une $\mathbf{Z}$-base $\mathscr{B}$ de Λ et une $\mathbf{Z}$-base $\mathscr{B}'$ de Λ' telles que les deux matrices de Gram G et G' associées à ces deux bases soient égales.

(b) Montrer que les deux propriétés suivantes sont équivalentes :

i. Λ et Λ' sont semblables.

ii. il existe une $\mathbf{Z}$-base $\mathscr{B}$ de Λ, une $\mathbf{Z}$-base $\mathscr{B}'$ de Λ' et un réel μ strictement positif tels que si G et G' sont les deux matrices de Gram associées à $\mathscr{B}$ et $\mathscr{B}'$ alors on a $G' = \mu G$.

(c) Pour tout réseau Λ on pose :

$$\Gamma_n(\Lambda) = m(\Lambda)^2 (\det \Lambda)^{-\frac{2}{n}} .$$

Démontrer que si Λ et Λ' sont semblables, alors $\Gamma_n(\Lambda) = \Gamma_n(\Lambda')$ et $\operatorname{Card} S(\Lambda) = \operatorname{Card} S(\Lambda')$.

– Partie C : Quelques exemples de réseaux –

On note, dans cette partie, $\mathscr{E}_n = (\varepsilon_1, \ldots, \varepsilon_n)$ la base canonique de $\mathbf{R}^n$, que l'on munit de sa structure euclidienne usuelle.

1. Le réseau $\mathbf{Z}^n$. On désigne par $\mathbf{Z}^n$ le réseau dont une $\mathbf{Z}$-base est $\mathscr{E}_n$.
Calculer $\det \mathbf{Z}^n$, $m(\mathbf{Z}^n)$, $S(\mathbf{Z}^n)$ et $\operatorname{Card} S(\mathbf{Z}^n)$.

2. Le réseau D_n. On suppose que $n \geqslant 2$, et on désigne par D_n la partie de $\mathbf{Z}^n$ définie par :

$$D_n = \{x = (x_1, \ldots, x_n) \in \mathbf{Z}^n \ / \ x_1 + \cdots + x_n \equiv 0 \bmod 2\}$$

(a) Montrer que D_n est un sous-groupe de $(\mathbf{Z}^n, +)$.

(b) On pose $e_1 = \varepsilon_1 + \varepsilon_2$ et $e_j = \varepsilon_j - \varepsilon_{j-1}$ pour $j \in \{2, \ldots, n\}$. Montrer que D_n est un réseau de $\mathbf{R}^n$ admettant $B = (e_i)_{1 \leqslant i \leqslant n}$ comme $\mathbf{Z}$-base.

(c) Calculer $m(D_n)$, $S(D_n)$ et $\operatorname{Card} S(D_n)$.

(d) Calculer $\det D_n$.

(e) Calculer la matrice de Gram associée à B.

(f) Montrer que D_2 est semblable à $\mathbf{Z}^2$. Donner une similitude f telle que $f(\mathbf{Z}^2) = D_2$.

(g) Montrer que, pour $n \geqslant 3$, D_n n'est pas semblable à $\mathbf{Z}^n$.

3. Le réseau A_2.
Soit H le plan de $\mathbf{R}^3$ d'équation $x_1 + x_2 + x_3 = 0$. On définit : $A_2 = H \cap \mathbf{Z}^3$.

(a) Montrer que $\mathscr{B} = (\varepsilon_2 - \varepsilon_1, \varepsilon_2 - \varepsilon_3)$ est une $\mathbf{Z}$-base de A_2, qui est donc un réseau de H.

(b) Calculer la matrice de Gram associée à $\mathscr{B}$.

(c) Calculer $m(A_2)$, $S(A_2)$ et $\operatorname{Card} S(A_2)$.

(d) i. Montrer que A_2 n'est pas semblable à D_2.

ii. Montrer que A_2 est semblable au réseau de $\mathbf{R}^2$ défini par $\Lambda = \mathbf{Z}u_1 + \mathbf{Z}u_2$ où $u_1 = (1,0)$ et $u_2 = (\frac{1}{2}, \frac{\sqrt{3}}{2})$ (on pourra utiliser la question 4b de la partie précédente).

iii. Justifier par un dessin l'appellation « réseau hexagonal » parfois donnée à Λ.

– Partie D –

1. On suppose dans cette question que $n \geqslant 2$. Soit Λ un réseau de E et b_1 un élément de $S(\Lambda)$. D'après la dernière question de la partie A, il existe une $\mathbf{Z}$-base $(b_1, u_2, \dots, u_n)$ de Λ contenant b_1, et, si p est la projection orthogonale de E sur $(\mathbf{R}b_1)^\perp$, $\Lambda' = p(\Lambda)$ est un réseau de $(\mathbf{R}b_1)^\perp$, dont $(p(u_2), \dots, p(u_n))$ est une $\mathbf{Z}$-base d'après la question **A-8**.

(a) Montrer que $\det \Lambda = \|b_1\| \det \Lambda'$.

(b) Soit un vecteur $x' \in \Lambda'$, et $x_0 \in \Lambda$ tel que $p(x_0) = x'$. On écrit $x_0 = \alpha b_1 + x'$, α étant un nombre réel.
Montrer qu'il existe un entier m tel que $(m - \alpha)^2 \leqslant \frac{1}{4}$.
On pose $x = x_0 - m b_1$; montrer que $x \in \Lambda$, que $p(x) = x'$, puis, en utilisant la propriété que b_1 est de norme minimum, que $\|x\|^2 \leqslant \frac{4}{3}\|x'\|^2$.

2. Soit Λ un réseau de E.

(a) Montrer qu'il existe une $\mathbf{Z}$-base $(u_1, \dots, u_n)$ de Λ telle que

$$\prod_{i=1}^{n} \|u_i\|^2 \leqslant \left(\frac{4}{3}\right)^{\frac{n(n-1)}{2}} (\det \Lambda)^2 \qquad (1)$$

(on pourra raisonner par récurrence sur n).

(b) En déduire l'inégalité :

$$m(\Lambda)^2 \leqslant \left(\frac{4}{3}\right)^{\frac{n-1}{2}} (\det \Lambda)^{\frac{2}{n}}. \qquad (2)$$

Par l'inégalité (2) on a : $\Gamma_n(\Lambda) \leqslant (\frac{4}{3})^{\frac{n-1}{2}}$. La borne supérieure des nombres $\Gamma_n(\Lambda)$, Λ parcourant l'ensemble des réseaux de E, est donc définie ; on la note γ_n. D'après ce qui précède, $\gamma_n \leqslant (\frac{4}{3})^{\frac{n-1}{2}}$.

3. (a) Montrer que $\gamma_2 = \frac{2}{\sqrt{3}}$ (on pourra considérer le réseau A_2).

(b) Réciproquement, soit un réseau Λ d'un espace vectoriel euclidien E de dimension 2, tel que $\Gamma_2(\Lambda) = \frac{2}{\sqrt{3}}$. On se propose de montrer que Λ est semblable au réseau A_2.

i. Justifier le fait qu'on peut se ramener au cas où $m(\Lambda) = 1$, ce que l'on suppose désormais.

ii. Soit (u_1, u_2) une $\mathbf{Z}$-base de Λ vérifiant l'inégalité (1). Montrer que $||u_1|| = ||u_2|| = 1$ et que le déterminant de (u_1, u_2) dans une base orthornormale de E est égal à $\pm\frac{\sqrt{3}}{2}$.

iii. Conclure.

– Partie E –

Dans ce qui suit, E désigne un plan euclidien et (e_1, e_2) une base orthonormale de E.
Soit p un nombre premier, K le corps $\mathbf{Z}/p\mathbf{Z}$ et m un diviseur de $p-1$; on note $f_m : K^* \to K^*$ le morphisme de groupes multiplicatifs défini par $f_m(x) = x^m$.

1. (a) Montrer que, pour tout élément $y \in f_m(K^*)$, $y^{(p-1)/m} - 1 = 0$.

(b) En déduire que $\mathrm{Card}\, f_m(K^*) \leqslant \frac{p-1}{m}$, puis que $\mathrm{Card} \ker f_m \geqslant m$.

(c) En déduire que le polynôme $X^m - 1$ est scindé dans $K[X]$.

2. On suppose que $m = 4$.

(a) Déduire de la question précédente qu'il existe $u \in \mathbf{Z}$ tel que $u^2 + 1 \equiv 0 \mod p$.

(b) Soit Λ le réseau de E de $\mathbf{Z}$-base $(pe_1, ue_1 + e_2)$. Montrer que, pour tout $x \in \Lambda$, $||x||^2$ est un entier divisible par p.

(c) Montrer qu'il existe un vecteur non nul de Λ dont le carré de la norme vaut p (on pourra utiliser l'inégalité (2)).

(d) En déduire que, pour tout nombre premier $p \equiv 1 \mod 4$, il existe $a, b \in \mathbf{Z}$ tels que $p = a^2 + b^2$.

3. On suppose que $m = 8$.

(a) Montrer que le polynôme $X^4 + 1$ est scindé dans $K[X]$. En déduire qu'il existe $u \in \mathbf{Z}$ tel que $u^2 + 2 \equiv 0 \mod p$ (si z est une racine de $X^4 + 1$, on pourra calculer $(z - \frac{1}{z})^2$).

(b) En déduire que, pour tout nombre premier $p \equiv 1 \mod 8$, il existe $a, b \in \mathbf{Z}$ tels que $p = a^2 + 2b^2$ (on considéra le réseau de E de $\mathbf{Z}$-base $(pe_1, ue_1 + \sqrt{2}e_2)$).

4. On suppose que $m = 3$.

(a) Montrer que $X^2 + X + 1$ est scindé dans $K[X]$.
En déduire qu'il existe $u \in \mathbf{Z}$ tel que $u^2 + 3 \equiv 0 \mod p$.

(b) Soit Λ le réseau de E de $\mathbf{Z}$-base $(pe_1, ue_1 + \sqrt{3}e_2)$. Montrer que, pour tout $x \in \Lambda$, $||x||^2$ est un entier divisible par p, et que $||x||^2$ est soit impair, soit divisible par 4.

(c) En déduire que, pour tout nombre premier $p \equiv 1 \mod 3$, il existe $a, b \in \mathbf{Z}$ tels que $p = a^2 + 3b^2$.

———— FIN DU SUJET ————